REMARKS

The claims remaining in the present application are Claims 13-22 and 24-38. Claims 13-22 and 24-38 are rejected.

CLAIM REJECTIONS

35 U.S.C. §103(a)

Claims 13-16, 18-22, and 25-30

Claims 13-16, 18-22, and 25-30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent Application Publication 2002/0083344 by Vairavan, hereinafter referred to as the "Vairavan" reference in view of United States Patent No. 6,538,997 by Wang et al., hereinafter referred to as the "Wang" reference. Applicants have reviewed the cited references and respectfully submit that the present invention as recited in Claims 13-16, 18-22, and 25-30 is patentable over the combination of Vairavan in view of Wang for the following rationale.

Applicants respectfully direct the Examiner to independent Claim 13 that recites that an embodiment of the present invention is directed to (emphasis added):

> A computer-readable medium having stored thereon a program, which when run on a processor, performs a method of managing a network, said method comprising:
> comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses; and
> tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network.

Independent Claim 22 recites similar limitations. Claims 14-16 and 18-21 that depend from Independent Claim 13 and Claims 25-30 that depend from Independent Claim 22 provide further recitations of the features of the present invention.

Applicants respectfully submit that Vairavan does not teach, suggest, or describe, "comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses", as claimed (emphasis added). Instead, Applicants understand Vairavan to teach a networking device including a packet processor that can function as a network address translation (NAT) router ([0060]). The packet processor can also include a firewall module for providing security based on a security policy database ([0086]). Applicants understand the firewall module to implement different types of filtering algorithms for restricting access within a virtual private network (VPN) ([0086] through [0101]). Specifically, Applicants respectfully submit that the firewall module of Vairavan is not operable to "determine unexpected addresses" of received packets. Therefore, Applicants submit that Vairavan does not teach, suggest, or describe, "comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses", as claimed (emphasis added).

Furthermore, Applicants respectfully assert that Vairavan does not teach, describe or suggest "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added). Applicants understand Vairavan to teach that the firewall module may include a network intrusion detection mechanism that can detect misuse of a network by analyzing usage patterns for received packets ([0090]). In particular, Vairavan is silent as to tracing a topology of a network to determine a port with an unexpected address. Applicants have reviewed the Vairavan reference, and are unable to locate any teaching of tracing a network topology to locate a port with an unexpected address.

In contrast, the claimed embodiments recite a method of managing a network, including "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added). As described in the current specification, "[i]f the MAC address is not expected, then the topology is traced ... to find the host port 115 where the unexpected MAC address was learned, in step 450" (page 16, lines 21-23, emphasis added).

Furthermore, Applicants respectfully assert that the combination of Vairavan and Wang fails to teach or suggest the claimed embodiments because Wang does not overcome the shortcomings of Vairavan. Wang, alone or in combination with Vairavan, does not show or suggest either "comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses" or "tracing a topology of said network to determine a second port at which a packet associated with an unexpected address entered said network," as claimed (emphasis added).

Per applicants understanding, the Wang reference is silent in regard to "comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses", and therefore does not cure this deficiency of Vairavan.

Moreover, Applicants respectfully assert that Wang does not teach a system that traces a topology of a network to determine a port where a packet associated with said unauthorized address entered said network. In contrast, Applicants understand Wang to teach that a layer-2 trace can be used to gather general information related to the switched network or to gather specific diagnostic

information relating to a particular path through the switched network (Col. 6, line 18-21 of Wang). Per Applicants understanding, the traces taught by Wang are utilized to isolate or receive switch configuration information, to isolate frame loss problems, to trace a path between a sender and receiver, to discover information such as the maximum transmit units of a path, or to diagnose a problem with a specific path. See, e.g., col. 5, line 13 - col. 6, line 65. Per Applicants understanding, the above described "tracing" performed by Wang is for determining network efficiencies or diagnosing communications problems (i.e network maintenance). However, Wang does not teach or suggest tracing of the topology to determine the port where a packet associated with said unexpected address entered said network, as claimed.

Therefore, Applicants respectfully assert that nowhere does the combination of Vairavan in view of Wang teach, disclose or suggest the claimed embodiments of the present invention as recited in independent Claims 13 and 22, that these claims overcome the rejection under 35 U.S.C. § 103(a), and are thus in a condition for allowance. Applicants respectfully submit that the combination of Vairavan in view of Wang also does not teach or suggest the additional claimed features of the present invention as recited in Claims 14-16 and 18-21 that depend from Independent Claim 13 and Claims 25-30 that depend from Independent Claim 22. Therefore, Applicants respectfully submit that Claims 14-16, 18-21, and 25-30 also overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on allowable base claims.

Claims 17, 24 and 31-38

Claims 17, 24 and 31-38 are rejected under 35 U.S.C. §103(a) as being unpatentable over Vairavan and Wang in further view of United States Patent No.

5,805,801 by Holloway et al., hereinafter referred to as the "Holloway" reference. Claim 17 depends from independent Claim 13 and Claim 24 depends from independent Claim 22. Applicants have reviewed the cited references and respectfully submit that the present invention as recited in Claims 17, 24 and 31-38 is patentable over the combination of Vairavan in view of Holloway for the following rationale.

Applicants respectfully direct the Examiner to independent Claim 31 that recites that an embodiment of the present invention is directed to (emphasis added):

> A network comprising:
> a plurality switches;
> said switches interconnected and configured to control communication between a plurality of devices coupled to said network;
> a database having stored therein a stored physical topology of said network and authorized addresses associated with packets processed at ports of said switches, wherein said authorized addresses are based on said stored physical topology;
> a configuration agent that is able to program said switches based on said authorized addresses to detect a packet having an unauthorized address; and
> a management agent that is able to:
> compare addresses learned by said switches against said authorized addresses to determine an unauthorized address; and
> trace a topology of said network to determine a port where a packet associated with said unauthorized address entered said network.

Claims 32-38 that depend from Independent Claim 31 provide further recitations of the features of the present invention. Independent Claims 13 and 22 recite similar limitations.

Applicants respectfully assert that Vairavan does not teach, describe or suggest an ability to trace a topology of the network to "...determine a port where a packet associated with said unauthorized address entered said network," as claimed (emphasis added). Applicants understand Vairavan to teach that the firewall module may include a network intrusion detection mechanism that can detect

misuse of a network by analyzing usage patterns for received packets ([0090]). In particular, Vairavan is silent as to tracing a topology of a network to determine a port with an unauthorized address. Applicants have reviewed the Vairavan reference, and are unable to locate any teaching of tracing a network topology to locate a port with an unauthorized address.

Furthermore, Applicants respectfully assert that the combination of Vairavan and Wang fails to teach or suggest the claimed embodiment because Wang does not overcome the shortcomings of Vairavan. Wang, alone or in combination with Vairavan, does not teach, suggest, or describe an ability to trace a topology of the network to "...determine a port where a packet associated with said unauthorized address entered said network," as claimed (emphasis added).

In contrast, Applicants understand Wang to teach that a layer-2 trace can be used to gather general information related to the switched network or to gather specific diagnostic information relating to a particular path through the switched network (Col. 6, line 18-21 of Wang). Per Applicants understanding, the traces taught by Wang are utilized to isolate or receive switch configuration information, to isolate frame loss problems, to trace a path between a sender and receiver, to discover information such as the maximum transmit units of a path, or to diagnose a problem with a specific path. See, e.g., col. 5, line 13 - col. 6, line 65. Per Applicants understanding, the above described "tracing" performed by Wang is for determining network efficiencies or diagnosing communications problems (i.e network maintenance). However, Wang does not teach or suggest an ability to trace a topology of the network to "...determine a port where a packet associated with said unauthorized address entered said network," as claimed (emphasis added).

Furthermore, Applicants respectfully assert that the combination of Vairavan and Wang in further view of Holloway fails to teach or suggest the claimed embodiments because Holloway does not overcome the shortcomings of Vairavan and Wang which are detailed above. Holloway, alone or in combination with Vairavan and Wang, does not show or suggest an ability to trace a topology of the network to "...determine a port where a packet associated with said unauthorized address entered said network," as claimed (emphasis added).

In contrast, Holloway teaches that if the managed hub detects an unauthorized station connecting to the LAN, the hub disables the port and transmits a security breach detected frame (col. 3, lines 6-8). However, Holloway does not teach or an ability to trace a topology of the network to "...determine a port where a packet associated with said unauthorized address entered said network," as claimed (emphasis added).

Therefore, Applicants respectfully assert that nowhere does the combination of Vairavan and Wang in further view of Holloway teach, disclose or suggest the claimed embodiments of the present invention as recited in independent Claims 13, 22 and 31, that these claims overcome the rejection under 35 U.S.C. §103(a), and are thus in a condition for allowance. Applicants respectfully submit that the combination of Vairavan and Wang in further view of Holloway also does not teach or suggest the additional claimed features of the present invention as recited in Claim 17 that depends from independent Claim 13, Claim 24 that depends from independent Claim 22, and Claims 32-38 that depend from independent Claim 31. Therefore, Applicants respectfully submit that Claims 17, 24 and 32-38 also overcome the rejection under 35 U.S.C.

§103(a), and are in a condition for allowance as being dependent on allowable base claims.

CONCLUSION

In light of the above listed remarks, reconsideration of the rejected claims is requested. Based on the remarks presented above, it is respectfully submitted that Claims 13-22 and 24-38 overcome the rejections of record. Therefore, allowance of Claims 13-22 and 24-38 is respectfully solicited.

Should the Examiner have a question regarding the instant response, the Applicants invite the Examiner to contact the Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,

WAGNER, MURABITO & HAO LLP

Dated: 10/27/06

John P. Wagner, Jr.
Registration No.: 35,398

WAGNER, MURABITO & HAO LLP
Westridge Business Park
123 Westridge Drive
Watsonville, CA 95076
San Jose, CA 95113

Phone: (408) 938-9060
Facsimile: (831) 763-2895